Cyber Command chief warns of 'remote sabotage'

June 3 2010, by Chris Lefkow

General Keith Alexander, head of the newly created US Cyber Command, pictured in 2004, said Thursday that Pentagon networks are probed over six million times a day and expressed concern about a rise in "remote sabotage" attacks on computer systems.

The top US cyberwarrior said Thursday that Pentagon networks are probed over six million times a day and expressed concern about a rise in "remote sabotage" attacks on computer systems.

General Keith Alexander, head of the newly created US Cyber

Command, also said developing a real-time picture of threats to US military networks and the rules to fight back would be among the priorities in his position.

Alexander, who also heads the National Security Agency, the super secret US surveillance agency, said Pentagon systems are "probed by unauthorized users approximately 250,000 times an hour, over six million times a day."

In his first public remarks since assuming command of US Cyber Command two weeks ago, Alexander said the US military "depends on its networks for command and control, communications, intelligence, operations and logistics."

"We at the Department of Defense have more than seven million machines to protect linked in 15,000 networks," he said in a speech to cybersecurity experts and reporters at the Center for Strategic and International Studies.

"Today our nation's interests are in jeopardy," Alexander said citing "tremendous vulnerabilities" and threats from a "growing array of foreign actors, terrorists, criminal groups and individual hackers."

"Cyberspace has become a critical enabler for all elements of national and military power," Alexander said. "Our data must be protected."

The four-star general said denial of service attacks on Estonia and Georgia in 2007 and 2008 were aimed at temporarily shutting down computer networks but new threats have emerged.

"There are hints that some penetrations are targeting systems for remote sabotage," he said. "The potential for sabotage and destruction is now possible and something we must treat very seriously."

Alexander said the military and the government needed to increase their ability it see what is happening on computer networks in real-time.

"We have no situational awareness, it's very limited," he said. "We do not have a common operating picture for our networks.

"We need real-time situational awareness on our network to see where something bad is happening and take action there at that time," he said. "We must share indications and warning threat data at net speed."

Alexander also that more precise rules of engagement were needed over how to respond to cyberattacks on the United States.

"We have to establish clear rules of engagement that say what we can stop," he said.

"We have to look at it in two different venues -- what we're doing in peacetime and in wartime," he said. "Those things that you do in wartime, I think, are going to be different from what you do in peacetime."

A Russian proposal to create a cyberwarfare arms limitation treaty could be "a starting point for international debate" but "at levels above me," he said.

Alexander also said that the NSA, whose warrantless wire-tapping program has been ruled illegal by a US judge, takes civil liberties and privacy "very seriously" and is subject to strict oversight by Congress and the courts.

"We have a lot of lawyers at NSA," he said. "My responsibility as director of NSA is to ensure that what we do comports with the law.

"Every action that we take we have legal reviews of it all the way up or down," Alexander said. "I doesn't mean we won't make a mistake.

"The hard part is we can't go out and tell everybody exactly what we do because we give up capability that may be extremely useful in protecting our country and our allies," he said.

Citation: Cyber Command chief warns of 'remote sabotage' (2010, June 3) retrieved 10 April 2024 from https://phys.org/news/2010-06-cyber-chief-remote-sabotage.html